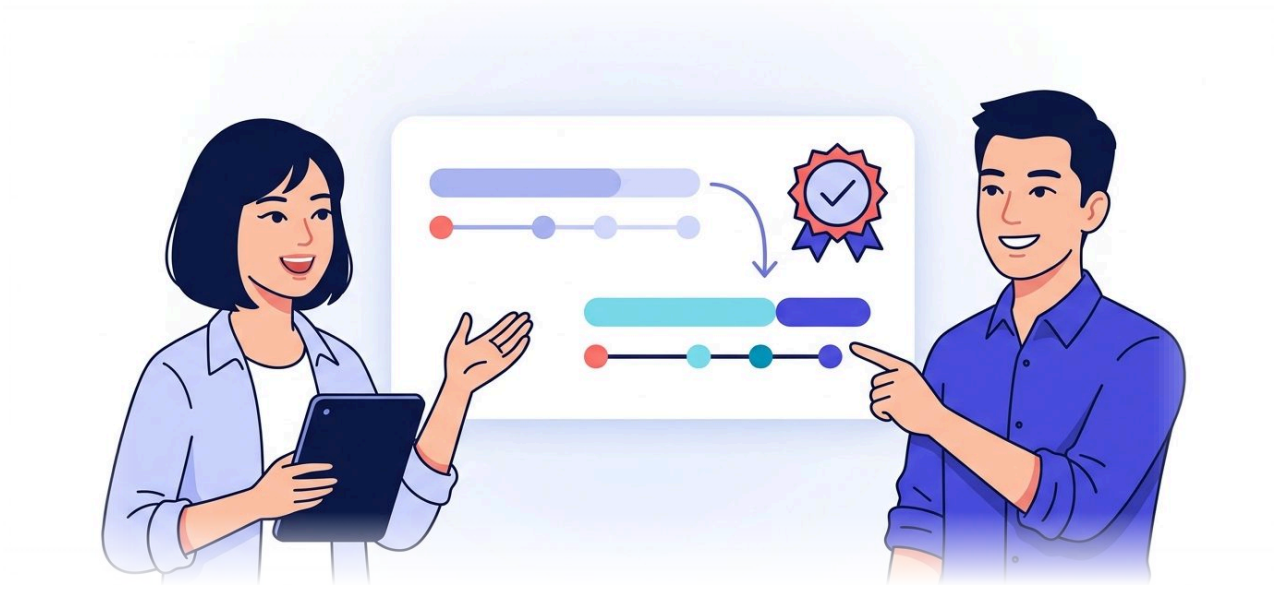
企业级智能体开发规约 v0.1

规定动作单据化、确认单九字段、R0–R4 定级标准、双轨停用退回、只追加审计账本与四级老系统接入。



09

个确认单强制结构化字段

R0–R4

五级规则网关硬性风险分级

L1–L4

老系统应用层接入优先顺序

发布机构

诺石数智

版本日期

v0.1 · 2026-11

适用角色

信息部 / 架构师 / 生态伙伴

官方网站

www.nerss.com

规范用词定义与文档结构

本规约定义诺石磐枢运行治理中枢及全部生态连接器的强制工程标准，确保智能体接入企业现有 ERP、OA、CRM 与 WMS 时权限可控、单据清晰、异常可退、审计可查。

规范用词约束级别

必须 强制工程条款，未满足禁止上线开放写回。

禁止 架构级绝对红线，须在网关与接口层硬阻断。

应当 推荐工程实践，偏离须在诊断报告中书面备案。

章节与核心交付物导览

第 1 章：动作单据化与九字段 JSON 规范
第 2 章：R0–R4 五级风险硬判定与 20 动作对照表
第 3 章：双轨自持与一键停用原界面退回
第 4 章：只追加审计账本与幂等防重规范
第 5 章：L1–L4 老系统接入顺序 + 空白动作登记卡

版本变更记录

版本号	发布日期	修订部门	主要修订说明
v0.1	2026-11	诺石架构与工程团队	首次公开发布完整动作单据化、R0–R4 定级、双轨退回、只追加账本与四级接入工程条款。

演示数据说明：本规约中出现的所有单号、确认单 JSON 与账本样例均为**演示数据 · 模拟示例，不代表真实运营或客户数据，**仅用于工程接口联调与字段规范示意。

1. 动作单据化与确认单九字段规范

1.1 禁止 严禁大模型通过黑盒工具调用直接修改存量业务系统正式状态，所有写入请求必须先被磐枢规则网关拦截。

1.2 必须 R2 级正式变更必须生成结构化确认单，清晰写明「办什么、改前改后、原文依据、回退方式、签字人、写回方式」六件事，缺少九字段中任一必填项网关拒绝放行。

1.3 必须 单条指令包含多项操作时，必须逐一拆分为独立动作分别定级（如 R0 查单 + R2 改交期 + R3 起草客户函）。

图 1 · 结构化确认单解剖与九字段强制清单 演示数据 · QR-20261001-0001



确认单标准 JSON 数据结构（演示示例）

```
{
  "slip_id": "QR-20261001-0001",                // 确认单唯一编号（演示数据）
  "idempotency_key": "erp-po-0032-v2-20261001", // 幂等防重键，防止重复写回
  "action_code": "erp.po.update_delivery_date", // 磐枢已登记动作编码
  "risk_level": "R2",                           // 规则网关硬判定，不由模型修改
  "target_system": "ERP-Main",
  "doc_id": "PO-20260918-0032",
  "diff": { "before": "2026-10-08", "after": "2026-10-15", "price_changed": false },
  "source_anchors": [
    { "type": "document", "ref": "供应商延期函(2026-10-01) 第2段" },
    { "type": "policy", "ref": "采购管理制度 v2.4 第4.3条" }
  ],
  "rollback_plan": "支持发起反向变更单；停用AI可带单号切回原ERP采购变更界面",
  "signer_role": "procurement_manager",
  "signature_ts": "2026-10-01T09:43:12+08:00",
  "receipt_id": "HZ-20261001-0001"              // 下游应用层接口写回回执
}
```

2. 五级风险硬判定与 20 项常见动作定级表

2.1 必须 所有动作风险等级须按企业内控制度在网关配置中写死，绝不由大模型依据上下文自行判断或降级。

2.2 禁止 未在磐枢动作注册表完成备案的动作请求，网关一律默认拦截并记录审计告警。

级别	制造与商贸常见业务动作	推荐接入通道	网关硬性放行方式	责任归属
R0	**采购订单原件查询**	ERP 只读接口	自动放行并记日志	经办人
R0	**备件实时库存查询**	WMS 只读视图	自动放行并记日志	经办人
R0	**制度与产品手册条款检索**	磐石底座	自动放行并附出处	经办人 / 访客

级别	制造与商贸常见业务动作	推荐接入通道	网关硬性放行方式	责任归属
R0	**三单（订单/出库/签收）拉取**	OMS + WMS	自动放行并记日志	售后经办人
R1	**差旅报销单制度合规初筛**	费控 / OA	生成内部标注草稿	财务审核人终审
R1	**标准合同条款偏差标注**	合同审批流	生成内部批注草稿	法务审核人终审
R1	**知识缺口工单起草**	磐石底座	分派骨干待审定	业务骨干
R1	**历史排障判例匹配建议**	磐石判例库	仅供调度参考草稿	调度长
R2	**修改采购订单到货交期**	ERP 官方接口	确认单签字后写回	采购主管
R2	**创建商贸售后补发单**	OMS / WMS 接口	确认单签字后写回	售后责任主管
R2	**下发现场异常派工单**	工单系统接口	确认单签字后写回	现场调度长
R2	**发起原 OA 审批流变更单**	OA 审批接口	确认单签字后发起	部门主管
R2	**发布审定后的知识条款升版**	磐石底座	审定人签字生效	知识管理员
R3	**起草发给客户的延期说明函**	邮件 / 企微草稿	AI 仅起草，人工发出	销售 / 客服负责人
R3	**起草采购或售后退款申请单**	财务系统草稿	AI 仅起草，财务办理	财务负责人
R3	**起草对外报价单与合同定稿**	商务文档草稿	AI 仅起草，人工发出	商务 / 法务
R4	**执行银行打款与资金划转**	禁止接入	网关硬性拒绝	AI 永不触达
R4	**直接读写或删除业务数据库**	禁止接入	网关硬性拒绝	AI 永不触达
R4	**修改员工账号、角色与权限**	禁止接入	网关硬性拒绝	AI 永不触达
R4	**向工业生产设备下发控制指令**	禁止接入	网关硬性拒绝	AI 永不触达

3. 双轨自持与 4. 只追加审计账本规范

3.1 必须 原系统人工界面必须永久保留；拨动「一键停用 AI」或模型超时异常时，自动将已识别的单号、字段与制度依据带入原系统表单，确保履约与审批保留连续的人工办理路径。

3.2 必须 AI 协同轨与原界面轨汇入同一条审批流与同一份审计账本，上线前须现场通过停用演练。

图 2 · 双轨并存与一键停用 AI 应急退回机制

同一审批流 · 同一审计账本



4.1 必须 审计账本按顺序只追加记录「意图发起、原件核验、主管签字、写回回执」四类事件，附加前序哈希校验链，禁止修改或物理删除。

4.2 必须 所有写回动作必须附带唯一幂等防重键与制度版本号快照；支持按单号一键导出 CSV / JSONL。

```
{
  "event_id": "EVT-20261001-00984",              // 只追加账本事件号（演示数据）
  "prev_hash": "sha256:8f2a9c...e104",           // 前序事件哈希，防事后篡改
  "trace_id": "TR-PO-20261001-0032",
  "stage": "writeback_receipt",                  // intent | verify | sign | writeback_receipt
  "policy_version": "采购管理制度@v2.4",
  "operator_id": "U-1024",
  "signer_id": "M-0018",
  "idempotency_key": "erp-po-0032-v2-20261001",
  "downstream_receipt": "HZ-20261001-0001",
  "created_at": "2026-10-01T09:43:14+08:00"
}
```

5. 四级老系统接入顺序与读写边界

5.1 必须 按「L1 官方接口 → L2 原系统审批流 → L3 只读同步视图 → L4 有限界面自动化」严格排序选型，能用上一级绝不降级采用下一级。

5.2 禁止 任何接入级别均禁止直连存量业务系统底层数据库进行读表或写表操作，保护原厂维保与事务一致性。

5.3 应当 采用 L4 过渡兜底的动作应当在诊断清单中标明替换计划，随原系统接口开放逐步升级至 L1 或 L2。

级别	接入方式	适用系统与前提条件	安全与维保边界说明	写回模式
L1	**官方接口（首选）**	ERP / OA / CRM / WMS 原厂或二次开发标准 REST / WebService / OpenAPI 接口	最推荐形态：事务校验、权限与日志完全交由原系统自身管理，支持幂等防重与回执返回。	支持受控写回（须 R2 签字）
L2	**原系统审批流程**	泛微、致远、钉钉、企微等审批流发起接口与标准表单回调	智能体备好单据与依据后推送至原有审批流，不另起审批孤岛，沿用既有签审权责。	经原审批流流转生效
L3	**只读同步视图**	无写接口的老旧系统或高度敏感台账，经授权只读视图/导出接口同步快照	智能体完成跨系统核对、标出差异并生成标准确认单，由人工在原系统界面核对录入。	只读核验，零写入风险
L4	**有限界面自动化**	短期无接口但频次极高的封闭老旧客户端界面（仅作过渡兜底）	限定固定表单与受控视窗，仍须经确认单签字后执行，并随老系统升级逐步替换为 L1/L2。	过渡兜底，逐步替换

生态伙伴接口共建提示：金蝶、用友、SAP、泛微、致远等原系统侧官方接口封装与二开工作优先由客户既有实施商伙伴承接，接口契约遵循 OpenAPI 3.0 标准归客户自有。

附页：单场景业务动作登记卡（空白表单模板）

供客户信息部、业务负责人与诺石架构师在场景诊断阶段共同填写，完成动作拆解、风险定级与接口边界确认。

单场景业务动作登记卡 NERSS-SPEC-01 · 场景编号：_____

场景名称	**月均办理频次**
主责业务部门	**授权签字角色**
涉及存量系统	
引用现行制度及版本	

序号	动作名称与目标系统	风险级别	接入级别	签字/放行方式	原界面退回入口
01		R0/R1/R2/R3	L1/L2/L3/L4		
02		R0/R1/R2/R3	L1/L2/L3/L4		
03		R0/R1/R2/R3	L1/L2/L3/L4		
04		R0/R1/R2/R3	L1/L2/L3/L4		
05		R0/R1/R2/R3	L1/L2/L3/L4		
06		R0/R1/R2/R3	L1/L2/L3/L4		

R4 禁止项核对（必勾）： ☐ 确认不含打款/支付执行 ☐ 确认不申请业务库直连写账号 ☐ 确认不修改用户权限 ☐ 确认不直控生产设备

业务负责人确认：_____ 日期：____ 年 __ 月 __ 日

信息部接口复核：_____ 日期：____ 年 __ 月 __ 日

诺石架构师：_____ 日期：____ 年 __ 月 __ 日